Share | Next Post

ForbesBrandVoice Connecting marketers to the Forbes audience. What is this?
TECH 7/24/2014 @ 10:39AM | 6,866 views

Will Amazon's New Fire Phone Burn Users?

SymantecVoice
Symantec Contributor, Symantec
+ Comment Now + Follow Comments
By Candid Wüest

Amazon's Fire Phone runs on Fire OS 3.5, which is based on Android 4.2 (Jelly Bean) and Amazon says they are working on upgrading to Android 4.4 (KitKat). Since the Fire OS is a fork of the Android OS, it is uncertain how Amazon will proceed with major Android updates or patches moving forward. Even with updates and patches, most users tend to never bother with upgrading the OS on their mobile device, which can intensify the attack surface of the device.

3D illusion

The phone has a spotlight on multimedia and comes pre-loaded with

certain applications. In order to attain this, the phone's motion sensors are used in tandem with four special cameras on the front of the phone that follow the user's head movements to adjust the graphic to the current viewing angle. This may sound a bit disturbing, because it means that the phone is always capturing images of you, and, thanks to the infrared lights, this image capture also works in the dark. Luckily, the phone does not appear to save these photos, so your images should not be at risk of falling into the wrong hands.

Firefly technology

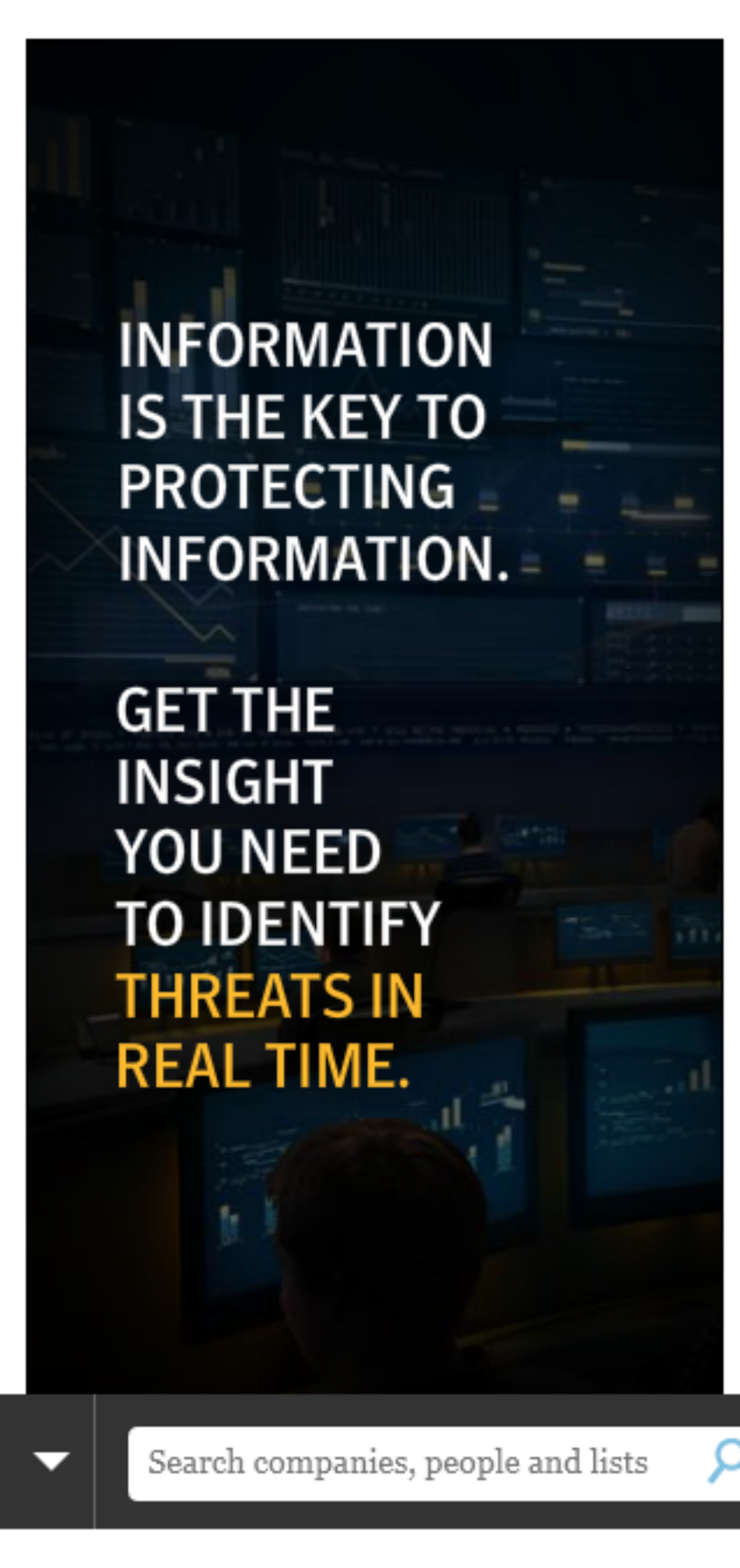
The Fire Phone's Firefly technology raises some apprehension about privacy and security. The Firefly service can recognize products, phone numbers, QR codes, URLs, and TV series after its user takes a picture of one of these items. Once the item is recognized, it is added to a list and can later be handled in many different ways. The most evident way is the option to purchase the identified merchandise on Amazon, but technology can link with streaming services and social media as well. Thankfully, there is not an option to purchase a product immediately after taking a photo, so users will not risk making an unintentional purchase after taking an accidental picture.

The Firefly service is accessible through an exclusive button on the lock screen, which also starts the camera. This is an important reason to not leave your phone unattended anywhere. Anyone could add undesirable items to your history list by taking photos. If errors in processing algorithm occur, they could cause crashes or configuration issues.

developers can create their own plug-ins, which means that they can also access the images and process them themselves. This presents some issues about privacy and as always users should be cautious when choosing which services to trust. In any case, it's probably better not to take photos of top-secret documents just to save a phone number.

No Google Play market

A great number of people have observed that the Amazon Fire Phone does not utilize the Google Play market. Rather, the phone supports Amazon's own app store, which has a good amount of apps, but is still missing a few user staples such as YouTube and Google Maps, for instance. Users who must have their favorite app are able to choose to install applications from untrusted third-party locations. Applications from these locations can contain malware that may lead to a compromised device. Even if an app from a third-party location is clean, it might not work because Fire OS uses a different framework than Google's Android OS. As with the Kindle Fire, this could lead to users rooting their Fire Phones to install the Google Play store. The heightened security on Amazon's devices means that there is no assurance of rooting a Fire Phone.



Silk browser

The Fire Phone uses the Amazon Silk Web browser, a custom built browser based on Chromium, that takes advantage of the Amazon cloud to process some content and decrease website load times. Privacy concerns regarding this feature have been noted, but there is an option to disable the Web proxy.

susceptibility than other browsers. It is not known if attackers will use the Amazon Silk browser to find any vulnerabilities in the software. The market distribution of the Fire Phone could affect this. Widespread distribution of the phone could offer an effective opportunity to attackers and entice them to put in the effort to find vulnerabilities.

There are still a few things that would be valuable in the next Fire Phone update. Features like integrated VPN or single-sign-on are on the wish list for the next Fire OS update and could help with any security issues.

As with any mobile device we advocate that users be cautious when installing apps from third-party markets and verify the privacy settings of their device.

Candid Wüest is Principal Symantec Threat Researcher based in Switzerland and active Symantec Connect blogger.

+ Comment Now + Follow Comments

Print | Report Corrections | Reprints & Permissions

ForbesBrandVoice Connecting marketers to the Forbes audience. What is this?
TECH 7/24/2014 @ 10:03AM | 2,250 views

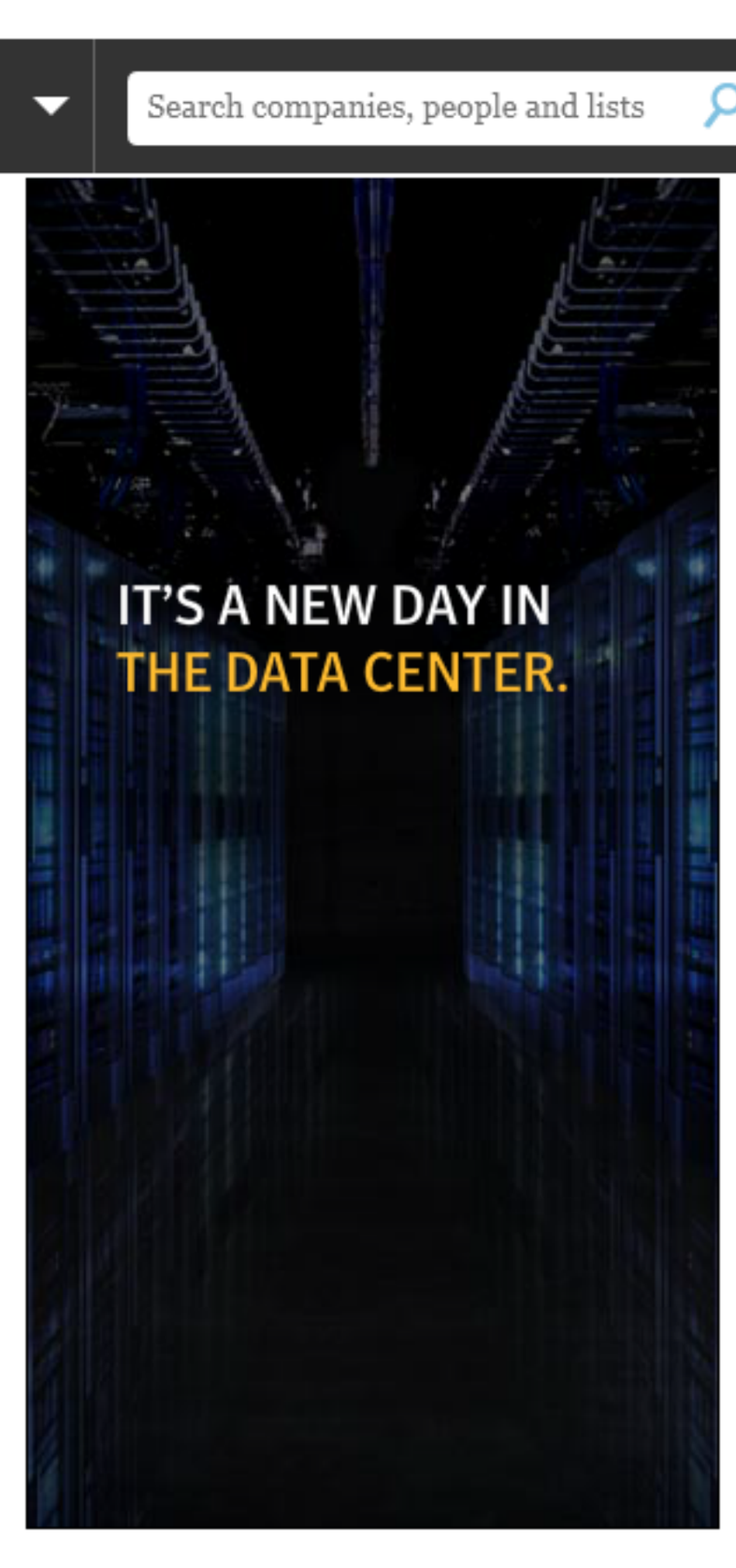
The 2014 Internet Security Threat Report: Year Of The Mega Data Breach

SymantecVoice
FOLLOW
Symantec Contributor, Symantec
+ Comment Now + Follow Comments

full bio →

Comment Now
+ Follow Comments

Symantec's Internet Security Threat Report (ISTR) reveals the latest findings about the current state of the threat landscape, based on our research and analysis from 2013. The research also disclosed more about the evolution of mobile malware and ransomware, and the possible threat posed by the Internet of Things. We'll examine each of these topics in greater detail below.



The year of the mega data breach

While 2011 was proclaimed by many as the "Year of the Data Breach," breaches in 2013 far exceeded previous years in size and scale. For 2013, we found the number of data breaches grew 62 percent from 2012, meaning that there were more than 552 million identities exposed last year – an increase of 368 percent. This was also the first year that the top eight data breaches each resulted in the loss of

Attackers set their sights on medium-sized businesses

Small and medium-sized businesses (SMBs) are key prey for attackers, and this year demonstrated no exception to the trend. In 2013, SMBs collectively made up more than half of all targeted attacks at 61 percent – up from 50 percent in 2012 – with medium-sized (2,500+ employees) businesses seeing the largest surge.

Attacks against businesses of all sizes and types grew, with an overall gain of 91 percent from 2012. Comparable to last year, cybercriminals launched watering hole attacks and spear-phishing to increase the effectiveness of their campaigns. Notwithstanding, spear-phishing campaigns were down 23 percent, with cybercriminals relying less on emails to carry out their attack campaigns. Watering hole attacks allowed the assailants to run more campaigns through drive-by-downloads, focusing on victims at the websites they frequently visit. Attempts were also aided by a 61 percent increase in zero-day vulnerabilities, which allowed attackers to set up on badly patched sites and infect their prey with little to no additional effort needed.

Government continued to be the most targeted industry (16 percent of all attacks). This year we examined not only the quantity of attacks but also who the preferred targets are and what the odds are of being targeted. The bad news is that no one faces positive odds and we all need to be apprehensive about targeted attacks. However, examining

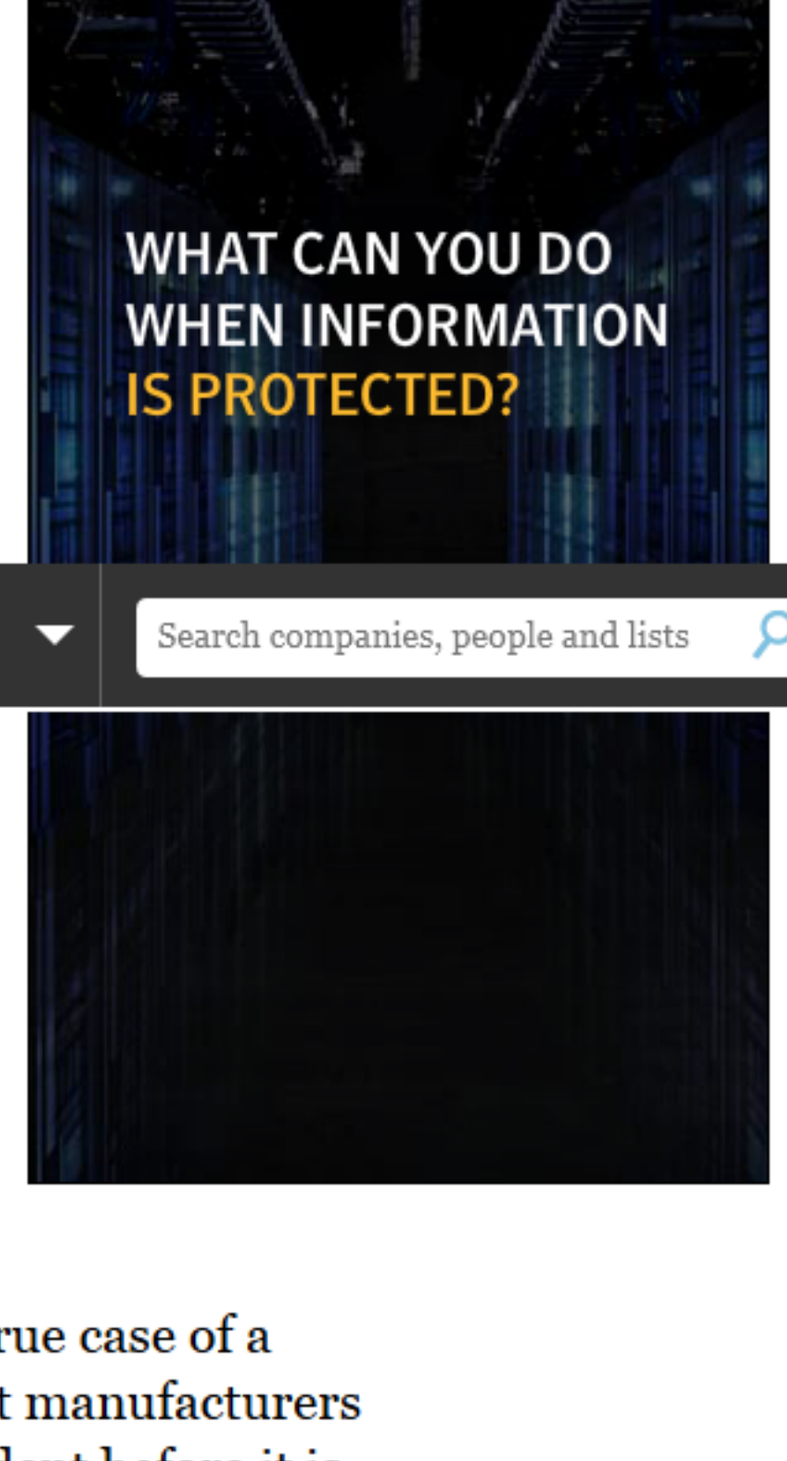
"most wanted" list of cyber targets.

Mobile malware and madware invades consumers' privacy

A multitude of people download new apps to their devices without a second thought, many malicious apps contain highly annoying or undesirable capabilities. Of the new malware threats created in 2013, 33 percent tracked users and 20 percent collected data from infected devices. 2013 also saw the first remote access toolkits (or RATs) begin to appear for Android devices. When installed and running on a device, these RATs can audit and make phone calls, read and send SMS messages, get access to the device's GPS coordinates, activate and use the camera and microphone and access files stored on the device – all without the awareness or authorization of the victim.

Ransomware growth explodes and turns even more vicious

As we had formerly predicted, ransomware, the malicious software that locks computers and files, grew swiftly in 2013. Ransomware saw an explosive 500 percent growth over last year and continued to be an extremely profitable enterprise for these attackers, netting $100 to $500 USD for each completed ransom payment. We also saw attackers become more savage by holding data hostage through high-end encryption and threatening to delete the information forever if the fee was not paid within the given time limit.



The future of identity theft: The Internet of Things

Which of these things do you think have been hacked in the past year: a refrigerator or a baby monitor? When asked this question, customers often reply, "Both." The correct answer is the baby

"never"; security researchers in 2013 established that attacks against cars, security cameras, televisions and medical equipment are all conceivable. The refrigerator's time will come. The Internet of Things (IoT) is on its way and related threats are sure to follow. In this year's report, we discussed what we've seen so far, and the general agreement is that the Internet connected device at most risk of attack today is the home router.

What comes next? With personal details and financial information being stored on IoT devices, it's only a matter of time before we find a true case of a refrigerator being hacked. Security is currently an afterthought for most manufacturers and users of these devices, and it will likely take a massive security incident before it is seriously considered. However, by starting the conversation now about the potential security risks, we will be that much more prepared when that day comes. This year's ISTR starts the conversation.

For more details, check out the complete Internet Security Threat Report, Vol. 19.

Kevin Haley is a speaker and blogger with expertise in protecting consumers against complex internet threats and other security risks.

+ Comment Now + Follow Comments

Print | Report Corrections | Reprints & Permissions

The 10 Richest American Athletes (Wall St. Cheat Sheet)
3 Steps to Become a Successful Trader (Trading for Newbies)
These 13 Dogs Are the Most Popular (Find the Best)
Olivia Palermo's Wedding Look (The Zoe Report)